Prosper Independent School District

Prosper ISD Data Governance Guidelines

Introduction

Prosper Independent School District (Prosper ISD or District) is committed to protecting the privacy of data that belongs to its students, families and staff. We take seriously the responsibility to maintain robust procedures and a secure network environment in order to mitigate the risk of compromising personal information.

With the integration between technology and teaching and learning, student and staff data are woven tightly into instructional platforms and information systems. Protecting personal data requires adherence to well-defined processes as well as communication and training for staff.

Support and execution of these guidelines will be a collaborative effort among leadership and departments that are responsible for staff and systems that manage District data.

These guidelines will be evaluated annually to ensure that the most current best practices are in place and are communicated to District staff and the community via publication of this document on the Technology department's web page.

Purpose

Prosper ISD's mission is to provide an educational system that maintains high expectations, provides quality instruction and establishes a safe, orderly learning environment. To that end, the Technology department ("Technology") maintains systems that enable teaching and learning for students and staff. In addition, Technology supports the administrative needs of the District for business operations and communication.

As the provider of innovative learning, the District becomes a steward of personal information for its students, families and staff. The purpose of these guidelines is to establish principles for the safe and secure collection, creation, management and storage of such information.

The intent of the Prosper ISD Data Governance Guidelines is also to promote the goals of board policy CPC (Records Management), CQ (Technology Resources), CQB (Cybersecurity), DH (Employee Standards of Conduct), and FL (Student Records).

Prosper ISD further maintains compliance with federal and state regulations including, but not limited to, the following:

- Children's Internet Protection Act (CIPA)
- Children's Online Privacy Protection Act (COPPA)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Protection of Pupil Rights Amendment (PPRA)
- Texas Education Code § 11.175 (School Cybersecurity)
- Texas Business and Commerce Code § 521.002; § 521.051; § 521.052; § 521.053
- Texas Government Code Chapter 552 (Public Information)

Finally, adherence to these guidelines supports the Texas Long Range Technology Plan Strategic Goal 4 (Safety and Security).

Data Access Guidelines

Data access shall be governed by role-based strategies as well as the principle of least privilege, ensuring that staff, vendors or other users granted rights to systems have only the privileges and level of access necessary for performance of their job or to meet the requirements of their responsibilities.

As staff are hired by the District, departments that manage information systems will determine the level of access to be granted based on job position. To the extent possible, identity management systems and automation will govern access rules in order to maintain established standards. Exceptions will be managed with the oversight of directors and executive level administration.

When staff are terminated, access to District email, file shares, cloud platforms, the student information system and any system integrated with identity management will automatically be revoked. Revoking access to any other system is the responsibility of that department and its director. Notifications of employee termination are provided to those administrators for that purpose.

Vendor or third-party access to District systems shall be created based on the principle of least privilege with expiration dates that reflect the expected scope of work. Regular audits shall be conducted to ensure that accounts are terminated in a timely fashion. Vendor or third-party access to district networks and systems will be monitored by Technology, but the ultimate responsibility for these parties lies with the department that contracts with them.

Data access is governed by the Prosper ISD Employee Responsible Use Policy, the Prosper ISD Employee Handbook, and Board Policy CPC, CQ, DH and FL.

Data Usage Guidelines

The expectation for data usage is that staff will appropriately protect personally identifiable information (PII) at all times.

PII is defined by the U.S. Department of Education as identifiable information that is maintained in education records and includes direct identifiers, such as a student's name or identification number, indirect identifiers, such as a student's date of birth, or other information which can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information.

PII should not be accessed except for authorized purposes or exposed unnecessarily either by hard copy, electronic communication, or storage on any type of device outside of a protected District system. Staff shall not move or copy PII. Any moves or copies will be handled by the data owners with guidance from the data steward, and not by general data users. Examples of this would be taking screenshots or copying data containing PII and storing it in department or personal network drives, Google drives, local hard drives, removable USB drives, etc.

Staff are provided with access to the District's virtual private network (VPN), and the expectation is that all staff members will utilize the VPN any time that student and/or staff data is accessed outside of the district's protected network.

Data usage is governed by the Prosper ISD Employee Responsible Use Policy, the Prosper ISD Employee Handbook, and Board Policy CPC, CQ, DH and FL.

Data Integration

Integration of Prosper ISD student, staff or District data with any application, platform or service shall be reviewed and evaluated by Technology in coordination with the stakeholder(s) requesting the integration.

Before any application, platform or service is purchased with District funds, Prosper Education Foundation funds, or other campus-related funds (i.e. PTO), the Software Request process shall be followed.

Through the Prosper ISD Software Request process, the potential application, platform or service shall be evaluated for instructional appropriateness, technical compatibility, and privacy compliance. Technology will communicate with the vendor to execute a Data Privacy Agreement. The request will be denied if a Data Privacy Agreement cannot be executed.

Once an application, platform or service is approved, Technology will work with vendors or third parties to implement secure authentication according to District standards and integrate data in a way that student and/or staff data can be maintained securely as well.

Upon termination of an agreement with a vendor or third party, Technology will negotiate the transfer or destruction of District data.

Data Integrity

The integrity of Prosper ISD data will be protected by secured network systems, including but not limited to firewalls with intrusion detection and prevention systems, network segmentation, email security systems, hardened operating systems, security logging and monitoring, cloud platform monitoring, and endpoint detection and response.

The District has an established Incident Response Policy that establishes roles and responsibilities for District executives and stakeholders. The Incident Response Plan outlines methodologies for responding to a variety of incident types. It includes a communication plan in the event of an incident that impacts staff, students and families. The District also maintains cyber security insurance which is reviewed annually.

Incident response and communication are governed by Board Policy CQB, Texas Education Code § 11.175 (School Cybersecurity) and Texas Business and Commerce Code § 521.002; § 521.051; § 521.052; § 521.053 (Personal Identity Theft).

Data Governance Team

Role	Responsibility
Chief Technology Officer	Oversight of inter-departmental collaboration; communication with executive cabinet; annual review process
Network Services Director	Oversight of network systems and services; management of information security policies
Cybersecurity System Administrator	Security policies and network system security
Data Integration System Administrator	Secure data integration standards; liaison with district stakeholders of various systems and vendors/third parties
District Services Director	Oversight of student information system, food services
Skyward System Administrator	Administration of student information system, including management of security
ERP Business Analyst	Support for human resources and business information systems
PEIMS Coordinator	Training and communication for campus registrars and other staff whose job responsibilities involve mandatory state reporting
Director of Program Evaluation & Curriculum	Oversight of special programs, including student information system requirements; management of policies and staff related to special programs
Health Services Director	Oversight of district nursing staff and management of health records
Special Education Coordinator	Oversight of Special Education information system; management of policies and staff related to Special Education
Human Resources Director	Oversight of human resource information system; management of policies and staff related to HR access
Business Services Director	Oversight of business management and financial systems; management of policies and staff related to business operations
Director of Curriculum & Instruction	Oversight of instructional applications and platforms; management of policies and staff related to curriculum and instruction
General Counsel	Legal compliance with federal and state regulations and board policy

Review Process

The Prosper ISD Data Governance Guidelines will be reviewed annually by the data governance team. As part of the review process, any updates to governing policies such as board policy and federal or state regulations will be considered and the guidelines will be modified or amended as necessary to stay in compliance.

In addition, any changes to data governance that may impact the Prosper ISD Employee Handbook or Employee and Student Responsible Use Policies will be taken into consideration so that those documents can be adjusted for the upcoming school year.

Finally, any changes in district technology standards, platforms, services, information systems, applications or best practices that require modification of these guidelines will be considered.

Updates to the Prosper ISD Data Governance Guidelines will be communicated to staff and published on the Technology web page.

Resources

The following policies and documents are referenced as governing these guidelines:

- Prosper ISD Board Policy
- Prosper ISD Employee Handbook
- Prosper ISD Employee Responsible Use Policy
- Prosper ISD Student Responsible Use Policy